A Silver Bullet? A Comparison of Accountants and Developers Mental Models in the Raise of Blockchain

Rose Esmander, Pascal Lafourcade, Marius Lombard-Platet, Claudia Negri Ribalta

A Silver Bullet? A Comparison of Accountants and Developers Mental Models in the Raise of Blockchain

Rose Esmander*
Department of Management Control, École Supérieure de Commerce de Paris (ESCP), Paris, France
Be-ys Research, Clermont-Ferrand, France
rose.esmander@almerys.com

Pascal Lafourcade
Université Clermont Auvergne, LIMOS CNRS UMR 6158, Aubière, France
pascal.lafourcade@uca.fr

Marius Lombard-Platet
DIENS, École normale supérieure, CNRS, PSL Research University, Paris, France
Be-ys Research, Clermont-Ferrand, France
marius.lombard-platet@ens.fr

Claudia Negri Ribalta†
CRI, Université Paris-1 Panthéon-Sorbonne, Paris, France
Be-ys Research, Clermont-Ferrand, France
claudia.negri@almerys.com

ABSTRACT

This exploratory paper intends to drive preliminary insights on the different mental models accountants and blockchain developers have on the implementation of blockchain for accounting. Based on the question of whether blockchain applications for accounting could be revolutionary, this paper employs a ground theory methodology based on semi-structured interviews and concept analysis to highlight the different approaches to transparency and trust between the selected groups, the challenges of blockchain and the potential effects of this technology in accounting. Although deeper studies are needed, the conclusions highlight the socio-technical nature of accounting; the relevance and changes of the concepts of trust and transparency when marrying both disciplines; and the real relevance of this technology for the processes of auditing and accounting.

KEYWORDS

accounting, blockchain, mental models, transparency, trust

ACM Reference Format:
Rose Esmander, Pascal Lafourcade, Marius Lombard-Platet, and Claudia Negri Ribalta. 2020. A Silver Bullet? A Comparison of Accountants and Developers Mental Models in the Raise of Blockchain. In *The 15th International Conference on Availability, Reliability and Security (ARES 2020), August 25–28, 2020, Virtual Event, Ireland*. ACM, New York, NY, USA, 10 pages. https://doi.org/10.1145/3407023.3409193

*Following theoretical computer science tradition, authors are listed in alphabetical order.
†Contact author.

The authors are thanking Manuel Parra Yagnam for his valuable input and remarks he made during the redaction of this paper.

ARES 2020, August 25–28,2020, Virtual Event, Ireland

ACM ISBN 978-1-4503-8833-7/20/08…$15.00
https://doi.org/10.1145/3407023.3409193

1 INTRODUCTION

Since its first implementation in 2009 [41], blockchain has become a buzzword and made headlines in all forms of scientific research and social media, all emphasazing its decentralization features. Moreover, its applicability is being tested in a wide range of fields, including finance [56], healthcare [2] and more. In fact, a recent study by consultancy firm has shown that for more than 52% of companies, blockchain is one of their top priorities [36]. However, companies also expressed concerns regarding certain elements in blockchain - such as regulations [8].

In mainstream media, blockchain has been advertised as the pinnacle of transparency and trust, and as a solution to many problems in those fields [16, 55]. Yet there appears to be little evidence to support these claims, most of them being simple iterations on the fact that blockchain is tamper-resistant. However, there has also been this vision of the blockchain as trust-less, given that all the information is present and there is no need to trust a central authority, such as banks.

This article is a interdisciplinary approach, which delivers preliminary results. We use the accounting realm as a use case for investigating these claims, as it has been widely acclaimed that blockchain will automate the accountant's job [14]. The objective of this study, first carried for a workshop on transparency and trust, is to carry out an exploratory research on the relationship between transparency, trust and blockchain in accounting. It particularly aims to start understanding:

(1) how blockchain may change mental models of trust and transparency;
(2) whether blockchain applications for accounting could be revolutionary or merely a "fashion-fad".

Our hypothesis is that accountants and blockchain developers have divergent mental models of transparency and trust, given their academic background. Given this divergence in mental models, the design and architecture of blockchain systems is directly impacted. Indeed, the accountant's system requirements of transparency and trust of don't necessarily align with what developers have in mind. However blockchain infrastructure for accounting (given the right parameters and characteristics) can, even with its failures, act as a support for accountants and auditors, enabling them to substantially minimize the issue of accessing a truthful source for accounting entries metadata

(e.g. who input the data, when, under which pretenses, etc) if requirements are correctly elicited. Since accounting is essentially a human process, blockchain based accounting will definitely not solve human mistakes in the accounting entries or the financial reports produced; nevertheless it will aid accountants in their job as a tool.

Our preliminary findings support this hypothesis. They also show that blockchain developers have a different mental model about transparency and trust compared to accountants, as their expectations on how blockchain can impact the accounting practice differs.

The papers is divided as follows. First, we explore related work, then in section Section 3 we expose the definitions use in our framework, as well as a statement of the problem. Then we expose our methodology for carrying the interviews, before presenting the results, and then analyzing them. Finally, we briefly discuss the limit of our study before concluding.

2 RELATED WORK

Blockchain can be a very powerful tool for storing data that is required to last over time. In other words, it is a tamper-resistant ledger, i.e. a database that resists modification. From an industry perspective, various professional services have reflected on how blockchain technology may impact different industries [8, 15, 19, 20]. Yet, academia has reacted slower to the phenomena. Only recently have other areas of study, apart from cryptography and computer science, started researching blockchain's impact. Some notable examples are Dai and Vasarhelyi [11], and Yermack [60] who have researched the potential impact of blockchain in financial services. The conclusions from both authors are similar: blockchain enables faster, cheaper and autonomous financial activities that are normally associated with a high time investment, such as balance sheets, fraud detection, storage of the data, *interalia*. This reflection coincides with the conclusion that professional services have on blockchain.

Blockchain could also potentially enable real-time accounting [11, 20, 60]. For example, auditors will be able to check every transaction made by a company and thus replace the current random sampling technique [19]. It could also allow for daily accounting data aggregation, creation and reporting, lowering risks for potential investors.

Similarly, Billing [8] surveyed over 600 executives in 15 countries and "found that 62% of the respondents have some blockchain project in development" . Yet, the same survey also highlighted that the three mains barriers to adopting blockchain are regulatory compliance, lack of trust from users and the ability of bringing networks together (each barrier being a preoccupation for more than 45% of the respondents).

Having built-in smart contracts to carry out the jobs that auditors were carrying before - such as cash flows or balance sheet - doesn't necessarily imply that the results are going to be lawful or trusted by other parties. As expressed by Deloitte [15], blockchain-based accounting systems will still require auditing to ensure that the system is working properly, and several other topics. For example, although it might be possible to see the (open) source code of the smart contract, it isn't always plausible to infer the behaviour.

Our research focuses on understanding how two particular requirements (transparency and trust) are perceived by the accountant. We then compare their mental models about transparency and trust with blockchain developers. With this data in hand, we try to understand how blockchain could potentially impact the these two requirements in the field of accounting. We carry out this research in an interdisciplinary manner, with a grounded-theory methodology. Our results are relevant for further development of blockchain systems, as stakeholders expectations play a key role in the adoption of said systems. To the best of our knowledge, this is the first time a systematic comparison between mental models of the users (here accountants) and the developpers is carried in the context of blockchain. As such, our study does not draw definitive conclusions, but rather preliminary results.

3 PRELIMINARIES

3.1 Transparency

Transparency is a concept that does not have a unified definition. There is vast academic research on its meaning and operationalization, yet no consensus on what it specifically means [39, 50]. It has been recognized that given the different conceptualizations of transparency, there has been an abuse of conceptual stretching [5, 39, 48]. It is thus important to clearly define transparency for this article.

There is unanimity that transparency is related to information and its disclosure. Different languages described transparency as an adjective for that something can be "seen through". Combining both conceptualizations, it is possible to conclude that at the very least transparency is about disclosure or access to information [4, 5, 39, 50].

However, the availability of information without an objective, context or substance, does not necessarily enable inferability about the object in question; i.e. it does not necessarily allow to "see through". That's why various authors have proposed that one key variable for transparency is information quality [28, 39, 43, 50]. As identified by [50] there is a research gap on a canonical definition of information quality, with divergent views between academics on whether this concept is tied to disclosure, clarity or accuracy of information.

We drawn upon this theoretical framework of transparency to define the working concept for this paper. We take "a three-dimensional model of transparency" that identifies it as a "perception of the quality of intentionally shared information from a sender and emphasizes that transparency is a function of information disclosure, clarity and accuracy" [50]. Disclosure means that the information available is relevant and shared in a timely way [50], available and accessible [28, 39]. By clarity, we refer to the inferability of the information [28, 39], being comprehended by the receiver [50], without industry terms [43] and understandable [McGaughey, 2002 in 50]. Finally accuracy means that the information is reliable, meaning that is hasn't been tampered with [28, 50].

These definitions are wide enough for being used in different cases without falling into conceptual stretching [48]. They allow for a clear analysis of transparency in accounting practice and blockchain implementations, as their focus is on the information rather than solely on the means on how information is distributed.

Finally, the aforementioned concepts are intrinsically related and similar to the IFRS's CC5 and CC19 (standards in the accounting field) definitions of relevance, faithful representation, comparability, verifiability, opportunity and comprehensibility [32]. We have decided to work with a broader definition for trust and transparency since blockchain applications outreaches accounting.Therefore, restricting trust and transparency to the IFRS' conceptual framework will force us to overlook some of the issues with this technological application.

3.2 Trust

Similarly, trust is complicated to define [24]. Depending on the context, authors define and adopt various definitions of trust [35]. In addition most definitions of trust are based upon specific empirical testing rather than conceptual analysis [38].

In many cases, trust is defined as "a psychological state compromising the intention to accept vulnerability based upon positive expectations of the intention of the behavior of another" [10, 13]. Similarly Tomkins [57] examines the interaction between accounting information and trust in inter-organizational relationships and concludes that trust is "the adoption of a belief by one party in a relationship that the other party will not act against his own interests... with the absence of detailed information about the actions of the other party". According to Neu [42] trust is defined as "social and constitutive expectations common to all exchange participants and consists of process based, character based, and institutional based".

Giddens' work has been inspirational in the domain of trust in systems [25, 26]. According to the author, lack of information is a prime requirement for trust and therefore trust becomes confidence in the reliability of a person or system - regarding a given set of outcomes or events - where that confidence is expressed as faith in the correctness of abstract principles (technical knowledge). In this article, we follow Guiddens' [25, 26] definition of trust, complementing it with Neu's [42]; that's to say, trust is a human process, that sets expectation about the reliability on the other party actions, meaning they won't act against the other party's interest.

Based on these definitions, blockchain can be defined as a trust-free technology, given that all the required information is present, thus there is no need to rely on, have faith in, or take any risks. This concept of blockchain being trust-free was introduced and discussed by Greiner and Wang as well [29], and later challenged by Lustig and Nardi [37], as well as Fröwis and Böhme [23].

From a computer science perspective - particularly from security - other definitions are given for trust. The concept of "trusted user" or rather of "honest" user is defined as someone who will strictly follow the protocol and as such not try to take advantage of the data they receive [12]. On the other hand, a "malicious" user can deviate from the protocol as much as they like [3], for instance by changing values or impersonating other users . Between these two extremes, a variety of attackers has been described. The most common one is probably the semi-honest adversary: it is usually defined as a user which "correctly follow the protocol specification, yet may attempt to learn additional information by analyzing the transcript of messages received during the execution" [3]. While other adversaries exist (fail-stop, covert...), semi-honest adversaries are the most common in the literature. Hence, cryptographic protocols do not necessarily require a full amount of trust in the participating parties: they rather define what amount of trust they are willing to concede and build attack-proof (or attack-resistant) protocols on top of these assumptions. In this context, anonymity is not guaranteed in Bitcoin against a honest but curious adversary, even though solutions exist [30, 33].

3.3 Trust and Transparency in Smart Contracts

Smart contracts (programs whose execution does not rely on a trusted authority) were first proposed in 1990 [54]. While, in a blockchain, data are stored in the ledger, smart contracts are the part embedding the business logic. Though Bitcoin proposes a small set of nontrivial operations such as multisignature wallets, the first and most iconic blockchain with implementation of smart contracts is Ethereum [58].

Given that smart contracts execution can be replicated by anyone, the need of trust in correct execution is lifted in blockchain using smart contracts. Because smart contracts' code is publicly available on the blockchain, it is often easy to infer what a smart contract does, and test its correctness on one or several instances. Hence, smart contracts are often advertised as a solution for increasing transparency, in applications such as finance, notary tasks, or gaming [19, 22].

However, open-source does not imply that the code is certified to work as expected, thus contradicting the underlying criterion of accuracy. For instance, because of classical results about undecidability, it is impossible to build an algorithm certifying the behavior of every possible smart contract [47]. Incorrect execution can spawn from three different causes: a genuine bug, a malicious payload, or a correct smart contract, but following bad or ambiguous specifications.

While, to the best of our knowledge, there is no evidence of intentionally malicious smart contracts for the moment, the risk cannot be excluded. For instance, in the open-source community, there are many examples of malicious libraries [1, 9, 40]. Sometimes, the vulnerability is a hidden mathematical weakness in the protocol, making it hard to even detect the presence of said vulnerability. For instance, it is widely assumed [7] that the cryptosystem DUAL_EC_DBRG has been crafted by the NSA to embed such a vulnerability. Bugs in open-source code can also have critical repercussions, such as the undetectable Heartbleed attack in 2014 [18]. In the world of blockchain, the DAO hack caused a breach of 3 million Ether (then worth 54 millions euros) because of a previously undetected bug [17].

We furthermore remark that open-source code can also be obfuscated. In our framework, obfuscated code is not transparent, as it lacks clarity (inferability on the behaviour of the smart contract). More pragmatically, reverse engineering is a popular activity, and smart contracts do not qualify as an exception [31], which proves that some pieces of code can be obscure by design, even on blockchain.

On a similar note, some programs are precisely designed to lower information disclosure to its bare minimum with zero-knowledge (ZK) cryptography. ZCash [49] is a pioneering cryptocurrency in that domain, and has implemented a blockchain in which all transactions can be ZK. We remark that while we get the accuracy (users can deduce all transactions are valid), we do not get any information disclosure (we know nothing else than the validity of the transfers), nor clarity (ZK proofs are not made to be human readable).

Therefore, the notion of transparency in code cannot be immediately deduced by presence of open-source algorithms, even in blockchain. An effort to characterize the qualities that a smart contract should have in order to be considered as 'trustless' is made by Fröwis and Böhme [23]. Notably, they examine how the flow of execution must be protected, what guarantees must be held to certify integrity over time, and so on.

4 METHODOLOGY

Trust and transparency are two unclear concepts, which we have tried to narrow down and define in the previous section. Some scholars have already noticed this use of both words as buzzwords, even before the invention of blockchain [6, 46].

Given the nature of this study, we have carried out a qualitative research, based on semi-structured interviews. We defined our two study groups, chartered accountants and blockchain developers. Once the interviews were collected, the interviews were coded and analyzed. We then proceeded to compare the answers from both groups and understand their mental models of transparency and trust.

In grounded theory methodology, theoretical sensitivity - as outlined by Strauss and Corbin [52] - comes from literature review, professional experience and analytic processes that help the understanding of the phenomena. Therefore, in order to carry out this research and given the nature of the subject, an extensive literary review on the subject of transparency, trust and accounting and security in smart contracts was carried out. This literary review was done before the interviews were carried out.

Next, the grounded theory methodology requires opening the survey (or interview in this case) sample to diverse groups. We have identified these two group of actors as our groups of interest: chartered accountants and blockchain developers. We interviewed 13 chartered accountants and 14 blockchain developers. Both groups had various levels of experiences (we interviewed junior, mid and senior levels) for diversity reason. However, the level of expertise wasn't taken into account in our analysis. This is further discussed in threats to validity.

We decided to carry out semi-structured interviews to chartered accountants and blockchain developers, based on the theoretical sampling method, in which "researchers seek and sample data that informs their theoretical categories" [53, p. 375]. Semi-structured interviews were deemed the best method as it gave us enough control to compare answers but also giving us more latitude to ask interviewees about specific topics, based on their answers. "Theoretical sampling is a tool that allows the researcher to generate theoretical insights by drawing on comparisons among samples of data" [27, p.874]. We decided to carry out interviews, as we seek to compare our identified interest groups' views and mental models on transparency, trust and blockchain, to better understand why it is being suggested that trust and transparency will evolve as concepts and if there are disagreements between the groups about this. In addition, we seek to compare how they think blockchain might affect the accounting realm and whether if there is an agreement on the potentials of blockchain for data processing. Given this, interviews were deemed as the best data gathering method.

Furthermore, the article is a a preliminary research, given that there is a gap in the literature about the subject particularly from an interdisciplinary perspective. Ergo, given these conditions, it was preferable to gather qualitative data over quantitative data, to gain further insight of the phenomena. It also aims at opening a new area of research.

Lastly, semi-structured interviews were selected as a method, as the research has defined objectives. This allows us to compare the answers from the interest groups, with certain control. However, some freedom was given to the interviewees to express other opinions, in case unforeseen issues arise. We developed a set of questions that were asked to both groups. These questions where carefully designed, as to avoid any bias or have underlying suggestions. The interviews were recorded and transcribed with interviewees having no chance to prepare their answers beforehand. The questions can be found in the extended version of this paper online.We were careful not to guide respondents on their answers, and not make them feel uncomfortable while answering [34]. Furthermore, interviewees were not briefed about blockchain nor accounting before answering, as this allowed us to get a better insight of their own mental model. The interviews were voluntary, no compensation was given, the interviewees were explained their rights and the goal of the study and had to sign a consent form.

The interviews were then anonymized to prevent any biases during analysis. The transcribed text was afterwards analyzed by two of the authors, to identify key words that appear repeatedly through the interviews, main message, concepts, among others through the NVivo software. Our guiding questions when carrying out the axial coding were: What are the main ideas of the answer? What is the interviewee trying to say here? What does it mean when referring to - for example - transparency and what does it imply? Is it possible to break up in more concept what the interviewee is saying? How does the answer relate to our theorizing? The NVivo software helped us visualize easier the codes and patterns that appeared through our analysis. This grounded theory method identifies the open coding stage on the 3 stage of coding [52]. Through the open coding process, we kept a open mind regarding the concepts that the interviewees used and we were constantly comparing the transcripts with the other transcripts. In addition, the interviews were also analyzed and coded through NVivo to get more robust results about our analysis . In detail, as outlined by Scott and Usher [51, p. 89] we are utilizing coding and classifying our interview transcripts by inferring concept's significance, patterns and repetitions that develop. Once we have the codes from the interviews, we proceed to axial coding - the second stage of coding - were we combine and relate the codes identified through our open code to categorize them. Then we make these patterns explicit and we elaborate a set of categories that hold firm in the setting being examined; the third stage - selective coding - of grounded theory method of coding approach by [52]. We relate how the informant's terms associate to the theoretical ideas that we have developed, and how the same categories (for example transparency) have different codes between accountants and blockchain developers, affecting their mental model.

When selecting the sample of accountants, we defined that we were going to interview accountants from different sectors: financial, forensic, junior and senior, *interalia*. This implies a trade-off that gives us a better insight and saturation [44, 52] on the accountant group's mental model towards the subject of study at the expense of explanatory power.

From a developer perspective, the rarity of blockchain developers is a challenge. As a consequence, to compensate the possible low levels of confidence and to achieve partial levels of saturation, we also interviewed blockchain project managers (PM) and a security professor (prof.) involved in blockchain projects. We acknowledge this might have consequence in our results.

Given the shortage of research and academics working on blockchain outside the field of computer science and information systems, this article's conclusions should not be taken as conclusive robust findings. The idea of this paper is to validate certain hypotheses about the possible effects that blockchain might have in concepts such as transparency and trust in the limited context of accounting and compare the mental model of two different groups about the subject. It aims at opening the field understanding the blockchain effects on socio-technical issues.

We describe the questions asked. For page limit reasons, comments of these questions will be available on the online report.

- What is your definition of trust?

Interviewee	Source	Length
Dev. 1 and PM	Sample frame	25 mins
Dev. 2	Sample frame	22 mins
Dev. 3 and PM	Sample frame	29 mins
Dev. 4	Sample frame	24 mins
Dev. 5 and PM	Sample frame	27 mins
Dev. 6 and Prof.	Sample frame	20 mins
Dev. 7 and postdoc	Given by Dev. 6	25 mins
Dev. 8	Sample frame	12 mins
Dev. 9	Sample frame	21 mins
Dev. 10	Sample frame	20 mins
Dev. 11	Sample frame	20 mins
Dev. 12	Sample frame	15 mins
Dev. 13	Sample frame	43 mins
Dev. 14	Sample frame	17 mins
Dev. 15	Sample frame	Refused
Acct. 1	Sample frame	17 mins
Acct. 2 and prof.	Sample frame	35 mins
Acct. 3	Sample frame	28 mins
Acct. 4 and prof.	Sample frame	21 mins
Acct. 5	Sample frame	26 mins
Acct. 6	Sample frame	37 mins
Acct. 7 and 8	Sample frame	23 mins
Acct. 9	Sample frame	13 mins
Acct. 10	Sample frame	13 mins
Acct. 11	Sample frame	18 mins
Acct. 12	Given by Acct. 11	15 mins
Acct. 13	Given by Acct. 11	8 mins

Table 1: Interview details of developers and accountants, with their experience. Accountants 7 and 8 were answering together.

- "Blockchain isn't the end of trust, it is the future of trust". What is your opinion on that phrase?
- What is the link between blockchain and trust?
- What issues can blockchain address? How and why?
- What does the word transparency mean to you?
- Do you think blockchain will affect accounting? Why? How?
- What are the problems that the blockchain could address in the field of accounting? How?
- What has been your experience with non-blockchain people, when implementing blockchain systems? (devs only)
- What have been your problems when implementing blockchain systems? (devs only)

5 INTERVIEW RESULTS

We carried 27 interviews in total, whose respective summaries can be found in Table 1. The coding processed was done in NVivo. As expressed on the methodology section, we first carried out an open coding process which we then processed in axial coding, whose some of the results can be found in table 2 [1]. While doing the axial coding, we noticed that accountants tended to use the same concepts for referring to transparency and trust. This was not the case for the blockchain developers, who appeared to have more divergent codes to explain concept.

We now share our general results. Given the scope of this study and the variance of concepts introduced in the interviews, not all codes can be shared and we only disclose the main highlights.

From these results, we developed a simplified mind model representation, available in Figure 1.

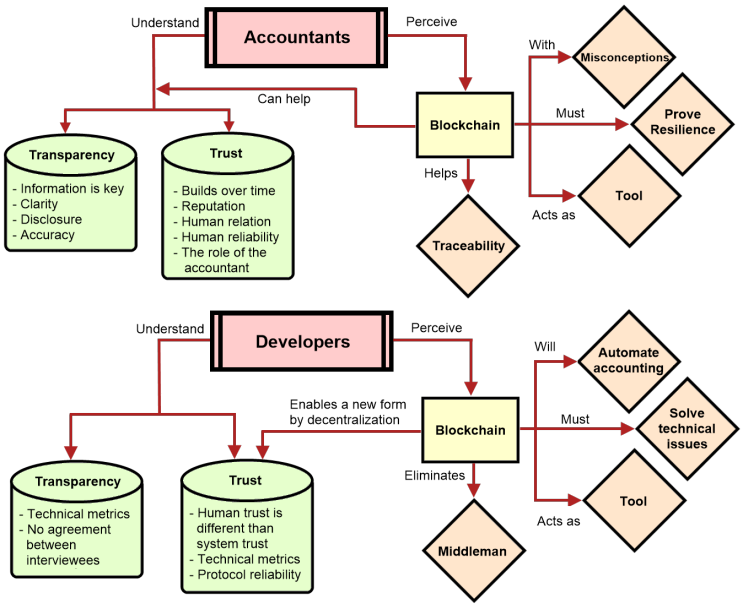

Figure 1: Simplified representation of accountants and developers mind models. For instance, accountants perceive that blockchain must prove its resilience.

5.1 Trust

Accountants. When it came to the mental model of trust, accountants gave elaborate descriptions and defined it as something that is more process based, that was situated in relation to a client, market or an organization. To accountants, trust was not simply quantitative in nature but rather qualitative, relating to reputation of the actor or accuracy of the information. The most identified code was reliability, discussed by 10 accountants, which they defined as them having certain expectations on the actions of another actor, the reputation of that actor or that the actions of the other actor were reliable. The second most identified code was accuracy, by 6 accountants, which they explained relates to information being complete, truthful, following standards or accurate (i.e ensuring that the data provided a good representation of the organization). Finally, a last element that was identified by 3 accountants, was the history of previous actions as being influential on their trust.

[1] Some example of the coding process. The following quote was coded as availability, reliability in *blockchain effects on accounting* "open the record like this [click] and you're going to have all the data. You'll be able to understand immediately". The next quote was coded as deletion of the middle-man in *blockchain effects on accounting* as it was an answer to the effects of blockchain in accounting question "accountability as a discipline should disappear. As a matter of fact, I find it impossible to justify why the profession still exists nowadays". Lastly, the next quote was another answer of the effect of blockchain in accounting and has been coded a availability, reliability, trust shift to technology, and requirements in *blockchain effects on accounting* "Blockchain is going to be the future of reliability, to the extent that you parameterize and style the information, and gives you the requirements necessary for you to trust this type of information"

Codes mentioned by not more than one accountant are traceability, difference between humans and computer trust and action delegation.

When prompted about the relationship of trust and blockchain, not all accountants gave answers, as 3 of them (Accountants #6, #10 and #13) couldn't see any relationship. From those who responded (a total of 10 answers) 7 accountants perceived blockchain as a way to improve trust. Their explanation included that tamper-proof nature of blockchain and traceability of data. However, 3 accountants highlighted that presently they don't trust this technology and that blockchain should first be adopted by the more influential companies to trust it. This relates with the idea of trust and reliability.

On another note, 3 accountants believe that blockchain can improve the transparency or efficiency of trust, explaining that they consider that blockchains systems give full access to data. When asked to explain how does transparency relates to trust, these accountants explained that blockchain gives them access to the history of data and ensures that the data has not been tampered with and it is accurate (which partially relates to our theorized model of transparency).

Developers. Unlike accountants, when asked about their definition of trust, 12 out of the 14 interviewed developers distinguished between trust in a person and trust in a system (see Table 2). When it came down to their trust in a person it was quite similar to what accountants said, highlighting reliability of the actor as critical (8 developers mentioning it) and historical experiences (5 developers mentioning).

The concept of reliability differs compared to accountants, as developers usually associate reliability as a property of the system rater than the participants. While it is important to verify the source of the data, verifying the authenticity of the participants was less important, because even if the participant were not honest, the system will not allow them to act in malicious ways (mentioned by 3 developers). Therefore, the trust of the developers is on the system, more specifically the code and the protocol (6 developers mentioned this attribution) .

11 developers mentioned blockchain provides trust in the data due to the decentralized nature of the technology (or the fact that it doesn't rely on a central authority). When asked to explain further, 6 developers mentioned the idea of traceability of information as granting trust and also that it is possible to trust that the code would execute correctly. In addition, 7 developers believe blockchain will create a new form of trust. For more information see Table 2.

Topic	Sub-topic	Accountants	Devs
Transparency	Information accuracy	9	6
	Information clarity	11	6
	Information disclosure	12	5
	Technical aspects	2	6
	Trust & transparency	5	6
Trust	Accuracy	6	3
	Reliability	10	8
	Human vs Computer trust	1	11
	History	3	5
Trust and blockchain	New form of trust	1	7
	Improves trust	7	2
	Trust more efficient or transparent	3	5
	Decentralization	1	11
Blockchain effects on accounting	Automatization	0	7
	Efficiency and speed	4	4
	Availability, reliability	7	4
	Elimination of middle-man	0	7
	Real time accounting	4	3
	Trust shift to technology	5	3
	Tamper-proof	4	3
	Tool	9	7
	Traceability	9	4

Table 2: Number of accountants and developers who evoked the given codes, for 14 developers and 13 accountants.

5.2 Transparency

Accountants. When asked about transparency, all the accountant cohort responded that it was related to information. The four main codes that accountants identified to be linked to transparency were information: clarity, accuracy, disclosure and trust. In fact, these patterns and tendencies can be seen in Table 2.

Accountants' definition of transparency falls in line with our literary review and theory about transparency. All but one accountant (Accountant #4), gave us a definition that relates to the disclosure of the information, and all but 2 accountants related clarity of information to transparency.

More specifically, 6 accountants explained that information should be "meaningful" (with this specific code) and another one explained that the information should refer to "how the algorithm works", highlighting that the sole access to information isn't a sufficient condition for clarity. Also, 9 accountants referred to accuracy as something they related to transparency. Furthermore, when asked directly about trust, no accountant safe one directly linked trust to transparency. Yet, when asked about transparency (*what's your definition of transparency*), 5 accountants did link it to trust. In addition, in answers to other questions accountants seemed to associate trust and transparency.

7 accountants talked about traceability of the information when explaining transparency yet they never said it was necessary for it.

In addition, in all our notes from most of the interviews, we noticed that accountants gave lengthy and detailed definitions of transparency.

Developers. In comparison, developers didn't relate transparency directly to information and manifested more divergent views on what it means. Some developers manifested to have similar views on the definition of transparency that we theorized (for example Developers #1 and #3) while others expressed definitions that relate transparency to trust (such as Developers #5 and #7). Indeed, most developers added other terms to explains their model of trust, which we cannot give here for page limit reasons.

6 developers mentioned several times that transparency can be provided based on the technical aspect of the system in use, with codes such as the system design, the protocol in usage, the knowledge on how the system works and even smart contracts. Other codes developers added about transparency were that the blockchain can allow transparency natively, verifiability, unlimited access to data or auditability (all mentioned by at most 2 developers, each time different).

From our notes, the definitions of transparency of most developers (except Developer #1 & project manager), were straightforward, short and concise. When asked to further explain the concept, they would repeat the same codes.

5.3 Effects of blockchain into accounting

Accountants. It is important to note that three accountants didn't answer these questions or couldn't relate accounting to blockchain. Particularly Accountant #6 didn't know anything about blockchain and Accountant #10 and #13 couldn't see any relationship, as they equated blockchain to cryptocurrencies. The two areas that that accountants perceived will be most affected , is the traceability of the information and blockchain acting as a tool, with 9 respondants identifying these areas (out of the 10 answers to theses questions). The second area agreed by most was that would help with the availability and reliability of information (which relates to transparency), with 7 answers.

Other concepts were mentioned, but in less frequency and were: shift of trust, efficiency and speed of information processing and tamper-proof information, shown in Table 2.

Our results show that most accountants have basics notions of blockchain and tend to relate it to cryptocurrencies. Some accountants had extensive and clear knowledge on the topic (Accountant #12), and others also but with strong misconceptions (Accountant #2 and Accountant #10, who only knew cryptocurrencies). Others didn't have extensive knowledge, but gave high-level and general answers.

Developers. From developers perspective, there was no agreement about which area blockchain systems would impact the most. None of the areas identified present more than 7 developers (see Table 2).

As per Table 2 the three concepts most identified are that blockchain will: automatize the accountant's practice, eliminate middleman (as a consequence of decentralization and smart contracts) and act as a tool. Other concepts, that were discussed are efficiency and speed, availability and reliability of the information, and traceability.

The challenges that blockchain system will have to overcome to become a widespread tool are - compared to what accountants identified - mostly technical obstacles. 13 developers acknowledged that technical (or technology) challenges are the biggest obstacle. For example, some of these challenges were the interaction with other systems, the consensus algorithms or developing a "fully fledged solution". Less than 33% of developers identified security and data management, privacy and regulations as challenges.

Finally, all the developers have expressed that it is difficult to explain the blockchain technology to non-blockchain enthusiasts, and whenever they were able to explain it, people would tend to overfantasize about the technical possibilities. Lastly, 5 developers said that non-blockchain enthusiasts tend to link blockchain to cryptocurrencies (which is correlated with the accountant's answer).

6 ANALYSIS AND FINDINGS

6.1 Trust

According to our results, trust is not a spontaneous event, it is something one builds over time. Developers made distinctions between trust in systems and trust in humans, while accountants' trust in systems was a byproduct of trust in human relations and other variables that were not directly related to the system itself. Both accountants and developers stated reliability as a requirement for trust. This aligns with the definition of trust provided by Giddens [25, 26]. However, developers made a distinction between the reliability for humans versus computers, being the area that developers agreed the most.

For accountants, to trust that full information was provided, they rely on their knowledge and on standards as well as qualitative data, such as historical relations and reputation of organizations to make judgements. Furthermore, one of the biggest determiners of reliability according to accountants is reputation. This was determined based on the context in which the object of trust is situated. On the other hand, developers reliability was embedded in the system itself to manage relationships between participants and ensure accurate communication between the different parties. For developers, their reliability was based on the functionality of the protocol and code that ensure that the system is doing what it is expected to do. The byproduct is a decentralized systems enabling consensus in a decentralized control environment. Based on this view, unlike accountants who place a high importance on relational trust, developers view authenticity of involved parties as secondary. In short, there exists a difference between developers and accountants in understanding what reliability conveys.

The accounting practice is seen to serves as a way of checking compliance to regulations, but also bring the added value of trust, provided by the human analysis to the data. This was reflected in the accountants' emphasis on vitality of their role in analysing and critiquing the data presented to them in order for them to deem it trustworthy. This aspect of interpreting data and telling a story could lead to another set of challenges which is the subjectivity of the accountant shaped by their own perceptions. While Porter [45] states that quantification is an important determiner of modernity and reproducibility of evidence and facts, and therefore trust, Fligstein [21] argues that quantification is embedded in political and economic arrangements that could lead to multiple interpretations of the same set of data based on the subjectivity of those telling the story using this data. In accounting practices this is the case, accountants are not just presenting numbers, they are telling a story using those numbers, and therefore they become controllers and producers of trust. It is no surprise then that the accountant's mental model of reliability and therefore trust is based on non quantitative and more subjective measures such as reputation, historical interactions and standards.

While developers did point out the importance of certifying the data that is entered into the system, which is done based on reputation of organizations feeding this data to the system, they viewed this as just one step of the trust building mechanism. Once the data is entered into the blockchain, trust is reduced to the characteristics of the blockchain: consensus, decentralization and tamper-proof. In this sense, building trust through relationships is no longer necessary, because the system manages them in such a way that encourages good behavior and makes it very difficult for one party to influence the system. By reducing the concept of trust to a attribute of a technology, the mental model of developers of trust is different to accountants, as the mechanisms for enabling trust differ, i.e. developers believe technology enables trust on its own, while on the other hand technology is perceived as a socio-technical issue by accountants.

In conclusion, both accountants and developers place a significant importance on reliability when deciding whether to trust or not, but each understand reliability differently. Accountants place their trust on the organizations to provide full information and use external factors such as accuracy of the information, reputation, historical data, whereas developers place their trust on the systems and their ability to properly execute functions and run protocol. Accounting is more than

just representing numbers, it is about analysing them in a given context, adding human value, which adds trusts to these data; explaining why accountant's highlighted elements such as reputation.Blockchain developers differentiate between trust in persons and trust in systems. They don't stretch the concept of human trust into system and have a different mental model, whereas the reduced to a protocol's ability to securely execute transactions as expected play a critical role.

6.2 Transparency

Based on our analysis and interviews, it seems that blockchain isn't expected to affect non-blockchain enthusiast's mental model of transparency, whereas also there is a different mental model of what transparency conveys to both groups. There is a disagreement between developers and accountants to what variables compose transparency. Notably, accountants mental model of transparency place information disclosure and clarity as the most important areas; i.e. that they have access to the full picture and that they are able to make conclusions about this information. These two areas aren't identified as critical by developers, in particular information disclosure.

Accountant repeatedly expressed that their job was to bring an "added" value to the information, implying that they require good quality information in order to produce robust conclusions about what they were analyzing. This remark is highly related to our three-dimensional theorization of transparency, were clarity on information is vital [28, 39, 43, 50]. On the contrary, clarity or quality wasn't present in most developers answers, as less than 50% of them related transparency to the quality of the information. This is problematical. Accountants are expecting information that allows them to give conclusions from accounting systems. However, blockchain developers don't put the same emphasis on information clarity . Thus, the parametrization of information is one of the key areas where blockchain developers and auditors are in misalignment. As Accountant #2 highlighted, parametrization of the information that will be available in the blockchain is the most important variable for the success of such systems.

Given that the core of accountancy is data analysis, it doesn't come as a surprise that accountants express their concerns over the nature of the data to be recorded on the blockchain systems. The features that could potentially make blockchain attractive to accountants, such as traceability, availability and reliability of information, will matter very little if the information recorded on the blockchain doesn't represent anything, isn't in the correct format, doesn't comply with legal requirements or in fact, the accountants don't trust it is truthful. To emphasise the importance of this, if the blockchain system isn't created without eliciting what type of information, in which format and - possibly - which standard to follow, auditors will find blockchain based tools of little help. Furthermore, blockchain based system will do very little for transparency, if developers don't put emphasis on information disclosure and clarity.

None of the respondents from the accountant group indicated that they thought blockchain might directly affect transparency.n m,The 4 developers that linked transparency and blockchain, focused on the idea of availability and traceability of the information, rather than the blockchain itself providing transparency. In other words, they hold the opinion that blockchain would increase - but not solve - the levels of transparency, as blockchain acts as a tool that helps in the area of information clarity of transparency and accuracy (as traceability gave them more confidence that the data was right). The importance is then on information and not on the systems design, architecture or technology. On the other hand, developers expressed that technical means on it owns could provide transparency regardless.

Thus, three working conclusions become apparent. Firstly, for accountants, transparency is related both to the availabiity and clarity (and quality) of information. The mental model accountants gave us is related to our theorized three-dimensional transparency definition. Secondly, parametrization of the information inside the blockchain will be one of the core issues when adopting those systems. It seems that this is one of the most important issues when adopting certain systems, though this conclusion requires further research. Which leads to the third conclusion: blockchain developers should elicit and understand the information requirements from the accountants. If the blockchain system fails to provide the type and format of information that accountants require, it might be difficult for blockchain-based systems to be adopted successfully. Moreover, accountants hint that blockchain - in their views - might increase the level of transparency based on how the information has been parametrized, indicating how important is for developers to understand the auditors' expectations.

6.3 Blockchain's impact of accounting

While it appears that blockchain is unlikely to change the concept of transparency on its own, consensus about its impact on accounting is not a clear cut, as accoutants' and developer's views are different.

All accountants except for three (Accountant #6, #10 and #13) reported that they believe that their field will be affected by blockchain. As previously mentioned, Accountant #6 explained it didn't know about blockchain and Accountant #10 and #13 couldn't relate cryptocurrencies to accounting (as their answers were based on cryptocurrencies) - and thus have been excluded from this discussion.

Firstly, as it happens, all developers raised that it was difficult for them to explain blockchain to non blockchain enthusiast. The reasons were: that people overfantasize about blockchain, they don't understand the technologies way of functioning and that they relate all blockchain technology to cryptocurrencies. We discovered through our interviews that accountants have a lot of misconceptions of blockchain and the ones that had some knowledge of it, overfantasized about it as expressed by the developers. The most common known feature by accountants was just immutability of the data and traceability, and there were concerning misconceptions about the capability of blockchain, particularly smart contracts. For instance, Accountant #2 perceived smart contracts as legally binding code. Moreover, Accountants #10 and #13 said that blockchain was only about cryptocurrencies. Intuitively, the area that mattered the most to accountants is the information that is going to be inside the blockchain. That is, in other words, how the parametrization of the information will be, which was highlighted Accountant #2. "*Blockchain is going to be the future of trust to the extent that you parameterize and style the information correctly [...] The only thing that is going to affect is the parameterization of the system, so that it delivers the information*" (excerpt from interview to Accountant #2). It further emphazises the importance of blockchain system being different ERP system, that developers need to work with accountants to see what they need (also mentioned by Accountant #8), certification process (also expressed by Accountant #4) and trust issues/sceptical.

In the same line, one of the most popular expected changes by accountants is traceability of data and aiding the accountants as a tool.Given that the most known feature of blockchain is the tamper-resistant nature of data, this might be the reason why they mention that records traceability will be the most impacted area.For example, auditing is normally carried out via a sampling technique, which is time-consuming and also leads to potential blindspots. Blockchain might potentially eliminate this task, by providing all available information on the system, explaining why accountants view it as a tool and helping with traceability. Furthermore, with the traceability of the correct data, accountants will be able to determine and deduce other types of information, such as compliance or even detect anomalies (such as fraud), elements brought up by more than half of the accountant. In other words, accountants recognize that blockchain can act a tool improving their efficiency, particularly improving the availability and reliability of the data and the efficiency of the data gathering process.

However, it is essential to acknowledge that availability and reliability is not guaranteed by blockchain per se, but rather by the underlying technology. Databases, and more generally computers, are available at any time and communicate with extreme efficiency. The need of a blockchain in a system is not always required, and its inherent complexity can even be a drawback. Especially, when data does not come from multiple sources, or that responsibility of the ownership of data is not disputed, then blockchain is not the best tool to use [59].

Hence, the accountant's views are that, blockchain will not bring "automatization" of the accountant's job, nor replace its' role, given that accountancy - as it has already been emphasized - it's bringing human value and interpretation to raw data. On a side note, some automatization features of accounting are already available in the market.

In a juxtaposition, developers have highlighted areas that accoutants have clearly pointed out that will no be affected. Particularly, the automatization of the accountant's job and the elimination of the middle-man. When talking about automatizaction with developers, didn't seem to realise that most of the features they mentioned already exist and are widely implemented through ERP software. Developers tend to believe that blockchain will revolutionize the field without having extensive knowledge of current accountability system and automatizations that are already out there. Likewise, half of developers thought that accountancy would in the future, be replaced by a blockchain system and eliminate the middle-man. They based their answers by stating that middle-men exists as a form of trust and given blockchain technological properties, this could be provided by the system itself. For example, Developer #10 expressed "*accountability as a discipline should disappear. As a matter of fact, I find it impossible to justify why the profession still exists nowadays*" or Developer #2 said "*I think blockchain can do a lot, especially in banking obviously insurance, loans, notaries, it can... uhm... short cut all the intermediaries*".

While blockchain is hailed by accountants as a promising tool, interviewees also insisted that blockchain must prove its resilience before being widely adopted in the public, to gain their trust. This conservative stance about new technologies stems from a precaution principle, as information reliability is one of the most important topics for accountants. It thus seems that before blockchain is adopted by the accounting ecosystems, two things must happen. The first one is a clarification of the role of blockchain and its possible use cases, in order to dissipate any misconception that accountants may have. The second one is the trial of time, where a blockchain based system must prove its efficiency and reliability before being handled any critical data.

This view differs dramatically from the one held by developers, whose main concern relating to blockchain is mainly focus on the programming process, regulations and security. This perspective from blockchain developers emerges as a natural differences from accountants, as their role in the software construction process is rather centered on the technical aspect of system. It further highlights the different mental models between developers and accountants regarding the effects of blockchain in accounting.

In this case, we can conclude that what accountants expectations from a blockchain system isn't shared or understood by the blockchain developers. By reviewing the answers from the blockchain developers, none of them mentioned the parametrization of the information or information issues and the only area they agreed on was by percieving blockchain as a tool.

7 THREATS TO VALIDITY

We recognize we have achieved high levels of saturation from both interviewed groups. The more accountants and developers we interviewed, the less new information we were finding. Indeed, in the last two interviewees of each group provided very little extra information. Furthermore, due to the general lack of blockchain developers in the market, we had to trade-off some control over our interviewees profile and interview project managers. Nevertheless, a bigger sample size would have given more robustness to our conclusion.

Given that our study is preliminary research with qualitative data, are conclusion should be treated as such, i.e. preliminary. Future research should focus in gathering more data and applying quantitative methods, to provide more robustness to the conclusion. Furthermore, variables such as levels of expertise and background/education details, among others, should be controlled in the future.

Also, other sources of data like meta-studies and analysis of real world projects might be interesting to explore. We recognize that there might be some biases in the answers, once again given the small number of respondents and the nature of our research methods.

Future research should focus on quantitative or mixed methods. Furthermore, future studies should aim at how the transparency and trust requirements of accountant's in blockchain system and propose prototypes or design of blockchain based accounting systems.

8 CONCLUSION

We have two outcomes: one, preliminary research results related to the understanding of blockchain technology in accounting and understand the different mental models of trust and transparency. Two, it has highlighted how the different mental models regarding trust and transparency can affect the requirement of a blockchain based system.

Furthermore, it seems that perception of transparency and trust aren't going to be greatly modified by the use of blockchain in accounting. There might be some evolution on these concepts as we discussed in this paper, but their core will remain the same.

Also, through our interviews analysis, we found that accountant's main concern regarding blockchain systems was the information that would be hosted inside the blockchain: how to minimize the issue of accessing an untruthful source for accounting entries metadata. This socio-technical issue is directly related to requirement engineering.

To conclude, further research should be carried out about blockchain implementation, accountancy and software engineering. In this context, we propose some future research questions and reflections that we believe will prove useful for this endeavor: what type of model is the best suited to gather requirements from all stakeholders if they do not have previous knowledge of the technology and developers say that it is difficult to explain? Can different mental models agree on the expectancy of software? What have been the key variables for the adoption of new technologies in accountancy?

REFERENCES

[1] Adam-npm. 2018. Reported malicious module: getcookies. https://blog.npmjs.org/post/173526807575/reported-malicious-module-getcookies

[2] C. C. Agbo, Q. H. Mahmoud, and J. M. Eklund. 2019. Blockchain Technology in Healthcare: A Systematic Review. *Healthcare (Basel)* (2019).

[3] Yonatan Aumann and Yehuda Lindell. 2007. Security Against Covert Adversaries: Efficient Protocols for Realistic Adversaries. In *Theory of Cryptography*.

[4] Carolyn Ball. 2009. What Is Transparency? *Public Integrity* (2009).

[5] Monika Bauhr and Marcia Grimes. 2017. Transparency to curb corruption? Concepts, measures and empirical merit. *Crime, Law and Social Change* (2017).

[6] Paul Beckmann, Karolina Gombert, Alexander Hoppe, Katharina Jautz, Miriam Lindner, Jessica Roome, Hanna Nicoló, Lara Schartau, Julia Schmälter, Tassilo Stiller, and Anne Theunissen. 2012. Transparency – more than a buzzword? (2012).

[7] Daniel J. Bernstein, Tanja Lange, and Ruben Niederhagen. 2016. *Dual EC: A Standardized Back Door*.

[8] Steve Billinghurst. 2018. "PwC global study shows four out of five executives (84%) surveyed report blockchain initiatives underway". https://www.pwc.com/im/en/media-room/articles/executives-have-blockchain-initiatives-underway.html

[9] ceejbot. 2017. 'crossenv' malware on the npm registry. https://blog.npmjs.org/post/163723642530/crossenv-malware-on-the-npm-registry

[10] Robert H Chenhall and Kim Langfield-Smith. 2003. Performance measurement and reward systems, trust, and strategic change. *Journal of management accounting research* (2003).

[11] Jun Dai and Miklos A. Vasarhelyi. 2017. Toward Blockchain-Based Accounting and Assurance. *Journal of Information Systems* (2017).

[12] Ivan Damgård, Oded Goldreich, Tatsuaki Okamoto, and Avi Wigderson. 1995. Honest Verifier vs Dishonest Verifier in Public Coin Zero-Knowledge Proofs. In *Advances in Cryptology — CRYPT0' 95*.

[13] Henri C Dekker. 2004. Control of inter-organizational relationships: evidence on appropriation concerns and coordination requirements. *Accounting, organizations and society* (2004).

[14] Deloitte. 2016. "Blockchain Technology. A game-change in accounting?". https://www2.deloitte.com/content/dam/Deloitte/de/Documents/Innovation/Blockchain_A%20game-changer%20in%20accounting.pdf

[15] Deloitte, Chartered Professional Accountant Canada, AICPA, and UWCISA. 2017. "Blockchain Technology and Its Potential Impact on the Audit and Assurance Profession". https://www.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/blockchain-technology-and-its-potential-impact-on-the-audit-and-assurance-profession.pdf

[16] Deloitte Insights. 2016. Blockchain: Democratized trust. https://www2.deloitte.com/us/en/insights/focus/tech-trends/2016/blockchain-applications-and-trust-in-a-global-economy.html

[17] Vikram Dhillon, David Metcalf, and Max Hooper. 2017. *The DAO Hacked*.

[18] Zakir Durumeric, Frank Li, James Kasten, Johanna Amann, Jethro Beekman, Mathias Payer, Nicolas Weaver, David Adrian, Vern Paxson, Michael Bailey, and J. Alex Halderman. 2014. The Matter of Heartbleed. In *Proceedings of the 2014 Conference on Internet Measurement Conference*.

[19] Ernst and Young Global. 2018. How blockchain will revolutionize finance and auditing. https://www.ey.com/en_gl/digital/blockchain-why-finance-and-auditing-will-never-be-the-same

[20] Financial Executive International. 2018. Blockchain for Financial Leaders: Opportunity vs. Reality. https://www2.deloitte.com/content/dam/Deloitte/us/Documents/financial-services/us-fsi-fei-blockchain-report-future-hr.pdf

[21] Neil Fligstein. 1998. The politics of quantification. *Accounting, Organizations and Society* (1998).

[22] Kristoffer Francisco and David Swanson. 2018. The Supply Chain Has No Clothes: Technology Adoption of Blockchain for Supply Chain Transparency. *Logistics* (2018).

[23] Michael Fröwis and Rainer Böhme. 2017. In Code We Trust? In *Data Privacy Management, Cryptocurrencies and Blockchain Technology*.

[24] Diego Gambetta et al. 1988. *Trust: Making and breaking cooperative relations*.

[25] Anthony Giddens. 1979. *Central problems in social theory: Action, structure, and contradiction in social analysis*.

[26] Anthony Giddens. 1991. *Modernity and self-identity: Self and society in the late modern age*.

[27] L.M. Given. 2008. *The Sage Encyclopedia of Qualitative Research Methods: A-L ; Vol. 2, M-Z Index*.

[28] Nelson Granados, Alok Gupta, and Robert J. Kauffman. 2010. Research Commentary—Information Transparency in Business-to-Consumer Markets: Concepts, Framework, and Research Agenda. *Info. Sys. Research* (2010).

[29] Martina Greiner and Hui Wang. 2015. Trust-free systems-a new research and design direction to handle trust-issues in P2P systems: the case of Bitcoin. (2015).

[30] Ethan Heilman, Foteini Baldimtsi, and Sharon Goldberg. 2016. Blindly signed contracts: Anonymous on-blockchain and off-blockchain bitcoin transactions. In *International conference on financial cryptography and data security*.

[31] @icchyr. 2018. Real World CTF 2018 Finals. https://blog.tonkatsu.info/ctf/2018/12/17/realworldctf-finals.html

[32] International Financial Reporting Standards Foundation. 2018. Conceptual Framework for Financial Reporting. https://www.ifrs.org/issued-standards/list-of-standards/conceptual-framework/#about

[33] Al Jawaheri and Husam Basil. 2017. *Deanonymizing tor hidden service users through bitcoin transactions analysis*. Master's thesis.

[34] Beth L. Leech. 2002. Asking Questions: Techniques for Semistructured Interviews. *PS: Political Science & Politics* (2002).

[35] Roy J Lewicki and Barbara Benedict Bunker. 1995. Trust in relationships. *Administrative Science Quarterly* (1995).

[36] Deloitte Development LLC. [n.d.]. Deloitte's 2019 Global Blockchain Survey.

[37] Caitlin Lustig and Bonnie Nardi. 2015. Algorithmic authority: The case of Bitcoin. In *2015 48th Hawaii International Conference on System Sciences*.

[38] D Harrison McKnight and Norman L Chervany. 2000. What is trust? A conceptual analysis and an interdisciplinary model. *AMCIS 2000 Proceedings* (2000).

[39] Greg Michener and Katherine Bersch. 2013. Identifying Transparency. *Info. Pol.* (2013).

[40] Andrej Mihajlov. 2018. Virus in eslint-scope? https://github.com/eslint/eslint-scope/issues/39

[41] Satoshi Nakamoto. 2008. Bitcoin: A peer-to-peer electronic cash system. http://www.bitcoin.org/bitcoin.pdf

[42] Dean Neu. 1991. Trust, impression management and the public accounting profession. *Critical Perspectives on Accounting* (1991).

[43] Andreas I. Nicolaou and D. Harrison McKnight. 2006. Perceived Information Quality in Data Exchanges: Effects on Risk, Trust, and Intention to Use. *Information Systems Research* (2006). http://www.jstor.org/stable/23015810

[44] Robert Pekkanen and Erik Bleich. 2013. *How to Report Interview Data*.

[45] Theodore M Porter. 1996. *Trust in numbers: The pursuit of objectivity in science and public life*. Princeton University Press.

[46] Martin Raiser. 1999. *Trust in transition*. Vol. 39.

[47] H. G. Rice. 1953. Classes of Recursively Enumerable Sets and Their Decision Problems. *Trans. Amer. Math. Soc.* (1953).

[48] Giovanni Sartori. 1970. Concept Misformation in Comparative Politics. *The American Political Science Review* (1970).

[49] E. B. Sasson, A. Chiesa, C. Garman, M. Green, I. Miers, E. Tromer, and M. Virza. 2014. Zerocash: Decentralized Anonymous Payments from Bitcoin. In *2014 IEEE Symposium on Security and Privacy*.

[50] Andrew K. Schnackenberg and Edward C. Tomlinson. 2016. Organizational Transparency: A New Perspective on Managing Trust in Organization-Stakeholder Relationships. *Journal of Management* (2016).

[51] D. Scott and R. Usher. 2011. *Researching Education: Data, Methods and Theory in Educational Enquiry*.

[52] Anselm Strauss and Juliet Corbin. 1990. *Basics of qualitative research: Grounded theory procedures and techniques.*

[53] Anselm Strauss and Juliet Corbin. 1994. *Grounded theory methodology: An overview.*

[54] Nick Szabo. 1997. Formalizing and Securing Relationships on Public Networks. *First Monday* (1997).

[55] Vince Tabora. 2018. How The Blockchain Can Bring Trust And Transparency To The Advertising Industry. https://medium.com/datadriveninvestor/how-the-blockchain-can-bring-trust-and-transparency-to-the-advertising-industry-467829cc161f

[56] Alex Tapscott and Don Tapscott. 2017. How blockchain is changing finance. *Harvard Business Review* (2017).

[57] Cyril Tomkins. 2001. Interdependencies, trust and information in relationships, alliances and networks. *Accounting, organizations and society* (2001).

[58] Gavin Wood. 2014. Ethereum: A secure decentralised generalised transaction ledger. (2014).

[59] Dylan Yaga, Peter Mell, Nik Roby, and Karen Scarfone. 2019. Blockchain technology overview. *arXiv preprint arXiv:1906.11078* (2019).

[60] David Yermack. 2017. Corporate Governance and Blockchains*. *Review of Finance* (2017).